IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

SAFELITE GROUP, INC.,

Plaintiff,

v.

Case No. 2:21-cv-4558
Judge Sarah D. Morrison
Magistrate Judge Elizabeth P. Deavers

NATHANIEL LOCKRIDGE, *et al.*,

Defendants.

OPINION AND ORDER

This matter is before the Court on Defendant Caliber Collision Centers (Caliber Holdings Corporation) d/b/a Caliber Auto Glass' ("Caliber") "Motion for Protection from Forensic Inspection of Defendant William Billingsley's Caliber-Issued Work Devices" (ECF No. 238), Plaintiff Safelite Group, Inc.'s ("Safelite") Response (ECF No. 242), and Caliber's Reply (ECF No. 245). Also before the Court is Safelite's "Motion for Leave to File Instanter Notice of Supplemental Evidence Supporting its Opposition to Caliber's Motion for Protective Order" (ECF No. 247) and Caliber's Response in opposition (ECF No. 248). For the reasons that follow, Caliber's Motion (ECF No. 238) is **GRANTED, in part,** and **DENIED, in part.** Safelite's Motion (ECF No. 247) is **GRANTED.**

I.

Initially, the Court turns to Safelite's motion for leave. (ECF No. 247.) According to Safelite, following the completion of the briefing cycle on Caliber's motion for a protective order, Safelite's expert completed a forensic examination of Billingsley's action on Safelite's network and email in the final days of his Safelite employment. Safelite explains that this

forensic examination revealed additional evidence of Billingsley's allegedly unlawful actions of which Safelite previously was unaware. Safelite has attached to its motion a declaration from Caleb W. Reyolds, a senior analyst for Interhack Corporation, a firm retained on Safelite's behalf to assist with forensic imaging. (ECF No. 247-1 at ⁋⁋ 1-3.) Safelite explains that Mr. Reynolds's examination determined that Billingsley deleted more than forty sent emails containing Safelite files and thousands of files and file folders. In response, Caliber claims that this evidence adds nothing relevant to the issues raised by its motion and Safelite's motion for leave should be denied. Caliber, however, has already addressed this additional information to some degree in its Reply in support of its motion after Safelite. (ECF No. 245 at 3-5.) Thus, Safelite's proposed additional information serves to provide context for the Court in considering the issues raised by Caliber's motion for a protective order. For this reason, Safelite's motion (ECF No. 247) is **GRANTED.**

II.

The Court has set forth the factual allegations of this case by way of background in previous orders and will not repeat them in detail here. Briefly, Defendant William Billingsley is a former Safelite employee now employed by Caliber. Safelite alleges that Billingsley and other Defendants violated enforceable non-compete and non-solicitation agreements, undertook a scheme to conceal their actions, and deleted relevant evidence. Among the claims Safelite asserts in the Second Amended Complaint are misappropriation of trade secret claims brought under federal, Ohio and Texas law and a state law spoliation claim. (Second Amended Complaint, ECF No. 126 Counts 1, 2, 4, and 16 against Billingsley.) These claims have survived a motion to dismiss. (Opinion and Order, ECF No. 229 at 26-27.)

The current motion relates to Safelite's request to forensically examine two devices: Billingsley's Caliber-issued phone and Caliber-issued laptop. Caliber retained Veracity, LLC, a

digital forensics firm, to perform an analysis of these devices and has submitted declarations from Jerry Hatchett, the Veracity employee who performed the forensic review. (ECF No. 238-3; 238-5; ECF No. 245-2.) Accordingly, Safelite explains that Caliber's production of "the forensic images already prepared by Caliber's expert as part of his examination would likely satisfy Safelite's request." (ECF No. 242 at 10.)[1]

III.

"District courts have broad discretion over docket control and the discovery process." *Pittman v. Experian Info. Sol., Inc*., 901 F.3d 619, 642 (6th Cir. 2018) (citation omitted). "'It is well established that the scope of discovery is within the sound discretion of the trial court.'" *Id*. (quoting *Lavado v. Keohane*, 992 F.2d 601, 604 (6th Cir. 1993)). The Federal Rules of Civil Procedure provide that "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case. . . ." Fed. R. Civ. P. 26(b)(1). While a plaintiff should "not be denied access to information necessary to establish her claim," a plaintiff may not be "permitted to go fishing and a trial court retains discretion to determine that a discovery request is too broad and oppressive." *In re Ohio Execution Protocol Litigation*, 845 F.3d 231, 236 (6th Cir. 2016) (citation omitted); *see also Gallagher v. Anthony*, No. 16-cv-00284, 2016 WL 2997599, at *1 (N.D. Ohio May 24, 2016) ("[D]istrict courts have discretion to limit the scope of discovery where the information sought is overly broad or would prove unduly burdensome to produce.").

The Federal Rules of Civil Procedure grant parties the right to "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense." Fed. R. Civ. P.

[1] As the Court understands it, Caliber was not able to obtain a forensic image of the Caliber iPhone because of the version of the mobile device management software downloaded. (ECF No. 238 at 7 n.3; ECF No. 238-5 at ¶ 3.)

26(b)(1); *see also Siriano v. Goodman Mfg. Co., L.P.*, No. 2:14-CV-1131, 2015 WL 8259548, at *5 (S.D. Ohio Dec. 9, 2015). "*Relevance* is construed very broadly for discovery purposes." *Doe v. Ohio State Univ.*, No. 2:16-CV-171, 2018 WL 1373868, at *2 (S.D. Ohio Mar. 19, 2018) (emphasis in original) (citation omitted)). Despite being construed broadly, the concept of relevance is not unlimited. *Averett v. Honda of Am. Mfg., Inc.*, No. 2:07-cv-1167, 2009 WL 799638, at *2 (S.D. Ohio March 24, 2009). Indeed, "[t]o satisfy the discoverability standard, the information sought must have more than minimal relevance to the claims or defenses." *Doe*, 2018 WL 1373868 at *2 (citations omitted). Furthermore, when information is "negligibly relevant [or] minimally important in resolving the issues" this will not satisfy the standard. *Id.* (citation omitted).

"[T]he Federal Rules of Civil Procedure instruct district courts to limit discovery where its 'burden or expense . . . outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.'" *Surles ex rel. Johnson v. Greyhound Lines, Inc.*, 474 F.3d 288, 305 (6th Cir. 2007) (quoting former Fed. R. Civ. P. 26(b)(2)(C)(iii)). This Court has previously held that "[t]hese factors are retained in revised Fed. R. Civ. P. 26(b)(1), reflecting 'their original place in defining the scope of discovery'" because "'[r]estoring proportionality' is the touchstone of revised Rule 26(b)(1)'s scope of discovery provisions." *Siriano*, 2015 WL 8259548, at *5 (citing Fed. R. Civ. P. 26(b)(1)). In analyzing the extent of the burden on the producing party, the Court of Appeals for the Sixth Circuit "has held that limiting the scope of discovery is appropriate when compliance 'would prove *unduly* burdensome,' not merely expensive or time-consuming." *Id.* (citing *Surles*, 474 F.3d at 305) (emphasis in original).

IV.

"A forensic image is an exact bit-for-bit duplication[ ] of a storage device. It does not alter anything on the original device, and is verifiable, meaning it uses hash values to confirm an exact bit-for-bit match." *List Indus., Inc. v. Umina*, No. 3:18-CV-199, 2019 WL 1933970, at *1 (S.D. Ohio May 1, 2019). As Caliber contends, the Court of Appeals for the Sixth Circuit has noted that forensic imaging should only be employed in limited circumstances. *Delta T, LLC v. Williams*, 337 F.R.D. 395, 400 (S.D. Ohio 2021) (citing *John B. v. Goetz*, 531 F.3d 448 (6th Cir. 2008)). The Sixth Circuit, however, also has recognized that forensic imaging "is not uncommon in the course of civil discovery." *John B.,* 531 F.3d at 459 (citing *Balboa Threadworks v. Stucky*, No. 05-1157-JTM-DWB, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006)). Indeed, courts "'have assumed that the provisions of Rule 34(a) concerning inspection, copying, and testing of tangible objects are sufficient to authorize a court to order reproduction of an entire hard drive using the 'mirror image' method.'" *Umina,* at *4 (quoting *Diepenhorst v. City of Battle Creek*, No. 1:05-cv-734, 2006 WL 1851243, at *2 (W.D. Mich. June 30, 2006)). Nevertheless, courts "have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature." *John B.*, at 459-60 (citing *Balboa Threadworks*, at *3). Thus, mere suspicion is not enough to justify a forensic imaging request. *Umina*, at *4.

Despite the above cautions, the current dispute does not require extensive analysis. Safelite alleges, in part, Billingsley's trade secret misappropriation under both federal and state law. In similar cases involving misappropriation claims, courts have permitted forensic imaging of electronic devices which may contain electronic data related to the alleged violation. *See*

Umina, 2019 WL 1933970, at *1; *Safety Today, Inc. v. Roy*, No. 2:12-CV-510, 2013 WL 1282384, at *5 (S.D. Ohio Mar. 27, 2013); *see also Ainstein AI, Inc. v. ADAC Plastics, Inc*., No. 23-2166-DDC-TJJ, 2023 WL 3568661, at *5 (D. Kan. May 19, 2023) (citing *Balboa Threadworks*, 2006 WL 763668, at *3); *IsoNova Techs. LLC v. OvaInnovations, LLC,* No. 20-CV-71-CJW-KEM, 2021 WL 7185227 (N.D. Iowa July 28, 2021) (citing *Balboa Threadworks* and ordering production of forensic imaging); *Strictly F/X L.L.C. v. Pyrotecnico F/X, L.L.C.,* No. 2:20-CV-00201-CCW, 2021 WL 2291826 (W.D. Pa. June 4, 2021) (ordering forensic imaging to be produced where expert's analysis of the forensic images was relevant to party's claims and within the scope of Rule 26(b)(1); *IHS Glob. Ltd. v. Trade Data Monitor LLC,* No. 2:18-CV-01025-DCN, 2019 WL 7049687 (D.S.C. Dec. 23, 2019) (recognizing that part of trade secret claim required plaintiff to show defendants used and misappropriated trade secrets and allowing inspection and copying of forensic image of laptop).

That is the straight-forward situation here. For example, taking only one aspect of Safelite's claims – its misappropriation claims, a relevant question is whether Billingsley used Safelite's information without authorization, *e.g.,* for Caliber's benefit. Safelite seeks to discover information directed to that issue through the requested forensic images. As Safelite further explains, "[t]he purpose of the forensic examination is to determine if documents Billingsley took ever made their way to his Caliber devices – whether or not they are still on the device." (ECR No. 242 at 13.) As Safelite correctly concludes, this evidence either will advance Safelite's claims by confirming that Safelite documents have been on the two Caliber devices at some point or will advance Caliber's position by confirming that they were not. (*Id.* at 11.) Thus, the connection between the Caliber devices and Safelite's claims cannot be said to be unduly vague or unsubstantiated.

Indeed, Caliber does not meaningfully challenge the relevance of the information sought by Safelite. Nor could it seriously do so, having undertaken the effort and expense of its own forensic examination of these devices. Instead, Caliber seeks to confuse the issue here by reframing Safelite's request as directed to "whether the Caliber devices were used to remove Safelite documents from Billingsley's Safelite laptop or transfer Safelite documents to Caliber." (ECF No. 245 at 2.) This mischaracterization ignores the possibility that Safelite documents made their way to the Caliber devices via other paths, including by way of Billingsley's initially e-mailing Safelite documents to himself at his personal Gmail account. This possibility, of course, goes to the heart of Safelite's claims of spoliation as supported, in part, by Billingsley's testimony regarding what the parties have deemed the "Bounce Back Email" and Billingsley's admitted deletion of that email and the surrounding timeframe. Caliber attempts to dismiss the significance of this possibility by asserting that its emails are stored on a server from which it already has produced more than 20,000 documents. As Safelite explains, however, emailed files could be renamed or deleted, permitting email activity to remain undetected absent a forensic examination.

Beyond this, Caliber seeks to preemptively foreclose Safelite's access to this information through its own forensic examination of the devices. Such an approach, however, runs contrary to the above-referenced authority. That is, in instances where courts have permitted forensic imaging, they have done so in a way that acknowledges the need for equal access to the information. *Umina*, 2019 WL 1933970, at *6 ("Defendants shall then provide List's computer forensic expert access to the hard drive, laptop computer, and desktop computer"); *Ainstein AI, Inc.,* 2023 WL 3568661, at *6 (directing parties to agree on outside, neutral third-party vendor and to establish an appropriate ESI protocol subject to court approval); *IsoNova Techs. LLC* ,

2021 WL 7185227, at *4 (directing defendants to produce the forensic images to Plaintiff's expert while specifically noting that defendants had retained an expert but sought to limit opposing party to use of a third-party neutral); *Strictly F/X L.L.C.,* 2021 WL 2291826, at *4 (directing that forensic images of the MacBook laptop issued by company defendant to former employee and of that former employee's personal external hard drive be produced to plaintiff's expert for examination in accordance with draft protocols provided to the Court by the parties); *IHS Glob. Ltd*., 2019 WL 7049687, at *5 (court appointed an expert witness pursuant to facilitate the inspection and copying of the laptop's forensic image to allow for plaintiff's inspection when defendants already had made a forensic image). Caliber offers nothing to the contrary beyond argument.

Finally, Caliber offers the conclusory argument that Safelite's request is overbroad. Neither party address this issue in a thoughtful way. For its part, however, Safelite maintains that an "Attorneys' Eyes Only" designation would address any of Caliber's concerns on this issue. Caliber does not argue that such a designation would not. On this sparse record, the Court agrees that an "Attorneys' Eyes Only" designation is appropriate. Caliber's motion will be granted to this limited extent.

Accordingly, Caliber's motion (ECF No. 238) is **GRANTED, in part,** to the extent that the forensic images already prepared by Caliber's expert as part of his examination are **DIRECTED** to be produced to Safelite for examination by Safelite's expert **WITHIN FOURTEEN (14) DAYS OF THE DATE OF THIS ORDER** subject to an **Attorneys' Eyes Only** designation as set forth in the parties' Stipulated Protective Order dated January 21, 2022 (ECF No. 84.) To the extent that a forensic image of the Caliber iPhone still has not been prepared due to technical difficulties, the parties will be expected to address this issue at the

conference scheduled for August 4, 2023, at 1:30 p.m. The motion is **DENIED, in part**, in all other respects.

IT IS SO ORDERED.

Date: July 25, 2023

/s/ Elizabeth A. Preston Deavers
ELIZABETH A. PRESTON DEAVERS
UNITED STATES MAGISTRATE JUDGE